(USAO GAN 6/10) Search Warrant

United States District Court

NORTHERN DISTRICT OF GEORGIA

In the Matter of the Search of

Property located at 4029 Mountain Side Trail, Dacula, GA 30019-7266

APPLICATION AND AFFIDAVIT FOR SEARCH WARRANT
Case number: 1:20-MC-833
UNDER SEAL

I, Paul Fike, being duly sworn depose and say:

I am a Special Agent of the Federal Bureau of Investigation and have reason to believe that in the property described as:

Property located at 4029 Mountain Side Trail, Dacula, GA 30019-7266, as further described in Attachment A (incorporated by reference),

in the Northern District of Georgia there is now concealed certain property and certain information, namely,

See Attachment B (incorporated by reference),

which constitutes evidence of a crime, contraband, fruits of crime, or items illegally possessed, and property designed for use, intended for use, or used in committing a crime, concerning violations of Title 18, United States Code, Section(s) 1344 and Title 18, United States Code, Section(s) 1956 and 1957. The facts to support a finding of Probable Cause are as follows:

SEE ATTACHED AFFIDAVIT

Continued on attached sheet made a part hereof.

Paul Fike
Signature of Affiant

Sworn to me by telephone pursuant to Federal Rule of Criminal Procedure 4.1

Paul Fike

May 8, 2020
Date

Atlanta , Georgia
City and States

CATHERINE M. SALINAS
UNITED STATES MAGISTRATE JUDGE
Name and Title of Judicial Officer

Catherine Salinas
Signature of Judicial Officer

AUSA J. Russell Phillips

Affidavit

I, Paul Fike, hereby depose and state under penalty of perjury that the following is true and correct to the best of my knowledge and belief:

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI"), and I have been so employed since 1996. I am currently assigned to the Atlanta Division investigating financial crimes, including wire fraud, mail fraud, bank fraud, and securities fraud. I am a law enforcement officer of the United States within the meaning of 18 U.S. C. §2510(7), and I am empowered by law to conduct investigations and to make arrests for federal felony offenses.

2. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from other law enforcement agents and various witnesses. Because this affidavit is being submitted for the limited purpose of establishing probable cause to obtain a search warrant, I have not included every detail of every aspect of the investigation. Rather, I have set forth only those facts that I believe are sufficient to establish probable cause for the requested search warrant. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

Premises to be Searched and Items to be Seized

3. The purpose of this affidavit is to set forth probable cause for the issuance of a search warrant pertaining to the property located at **4029 Mountain Side Trail, Dacula, GA 30019-7266**, which is the residence of Maurice Fayne, as further described in Attachment A, and all computers, electronic media and devices, and all closed and/or locked containers therein **("the Subject Premises")**.

4. The items to be seized from **the Subject Premises** are described in Attachment B.

Applicable Laws

5. The bank fraud statute, 18 U.S.C. § 1344, makes it a federal crime for anyone to knowingly execute or attempt to execute a scheme and artifice to defraud a financial institution, as defined in 18 U.S.C. § 20, or to obtain moneys and funds owned by and under the custody and control of a financial institution, by means of materially false and fraudulent pretenses, representations, and promises, and by the omission of material facts.

6. In addition, two money laundering statutes are applicable here:

   a. First, 18 U.S.C. § 1956(a)(1)(B)(i) makes it a federal crime to engage in a financial transaction, knowing that it involves funds that are the

proceeds of some unlawful activity, including bank fraud, if those funds were in fact the proceeds of unlawful activity, including bank fraud, and if the transaction was designed to conceal or disguise the nature, location, source, ownership, or control of the proceeds of the unlawful activity.

b. Second, 18 U.S.C. § 1957 makes it a federal crime to knowingly engage or attempt to engage in a monetary transaction, knowing that the transaction involved property or funds that were the proceeds of some criminal activity, including bank fraud, if the property had a value of more than $10,000, the property was in fact proceeds of that specified unlawful activity, and the transaction took place in the United States.

7. The CARES Act is a federal law enacted on March 29, 2020, designed to provide emergency financial assistance to the millions of Americans who are suffering the economic effects caused by the COVID-19 pandemic. One source of relief provided by the CARES Act was the authorization of up to $349 billion in SBA-guaranteed forgivable loans to small businesses through the Paycheck Protection Program (PPP). In April 2020, Congress authorized over $300 billion in additional PPP funding.

8. The PPP allows qualifying small-businesses and other organizations to receive loans with a maturity of two years and an interest rate of 1 percent. PPP loan proceeds must be used by businesses on payroll costs, interest on mortgages, rent, and utilities. The PPP allows the interest and principal to be forgiven if businesses spend the proceeds on these expenses within eight weeks of receipt and use at least 75 percent of the forgiven amount for payroll.

The Investigation

9. The United States Attorney's Office, the FBI, and the U.S. Small Business Administration, Office of Inspector General (SBA-OIG) are investigating a Georgia company called Flame Trucking, Inc. (Flame Trucking) and its owner, Maurice Fayne (Fayne).

10. On August 9, 2019, Fayne opened Account 1408 at United Community Bank Inc. (UCBI).

11. Fayne resides at **the Subject Premises**.

12. According to documents on file with the Georgia Secretary of State, Fayne owns Flame Trucking, and Flame Trucking's Principal Office is located at **the Subject Premises.**

13. On April 15, 2020, Fayne submitted a PPP Borrower Application Form (SBA Form 2483) to UCBI for his company, Flame Trucking. Based on the

representations that Fayne made and caused to be made on the SBA Form 2483, Flame Trucking received a PPP loan for $3,725,500. The loan proceeds were deposited into Fayne's UCBI Account 1408 on April 22, 2020. UCBI subsequently lowered the loan amount to $2,045,300.

14. To apply for this loan, Fayne signed and dated a PPP Borrower Application Form (SBA Form 2483) on April 15, 2020. On the form, Fayne reported to UCBI that Flame Trucking's average monthly payroll was $1,490,200. In support of this calculation, on April 24, 2020, an email was sent from flametruckinc@gmail.com to UCBI, attaching what Fayne represented to be the October, November, and December 2019 bank statements for Flame Trucking's account at Arvest Bank (account # 6977), titled in the name Maurice Fayne and Flame Trucking.

15. According to Arvest Bank, the account ending in 6977 is connected to Fayne's Social Security Number.

16. Arvest Bank informed investigators that the account ending in 6977 was closed on September 17, 2019.

17. Investigators provided Arvest Bank with copies of the October, November, and December 2019 bank statements that Fayne submitted or caused to be submitted to UCBI to support Flame Trucking's PPP loan application, and

Arvest Bank informed investigators that those monthly statements were not generated by Arvest Bank. In other words, they are fraudulent.

18. Page two of the SBA Form 2483 includes a list of certification statements that must be initialed by the borrower. Fayne initialed all of the certifications, including the one that reads as follows: "The funds will be used to retain workers and maintain payroll or make mortgage interest payments, lease payments, and utility payments, as specified under the Paycheck Protection Program Rule; I understand that if the funds are knowingly used for unauthorized purposes, the federal government may hold me legally liable, such as for charges of fraud." Fayne signed and dated SBA Form 2483 on April 15, 2020.

19. According to information provided by UCBI to the FBI on April 24, 2020, "Flame Trucking receive a PPP loan . . . this week and immediately began wiring funds from the account, 6 of which went to individuals." The information also listed eight suspicious wire transfers, including the following:

    a. REF #20201140054400 - $30,000 TO DANIEL E JAY – POW [purpose of wire]: PAYMENT ON LOAN

    b. REF #20201140054700 - $50,000 TO MICHAEL SARGENT – POW: PAYMENT ON LOAN

c. REF # 20201140020400 - $350,000 TO CAWANZA WILKINS – POW PAYROLL NORTH

20. Loan payments are not an authorized use of PPP funds under the CARES Act. *See* Federal Register /Vol. 85, No. 76 /Monday, April 20, 2020 /Rules and Regulations.

21. On May 6, 2020, Fayne was interviewed by federal law enforcement agents. Fayne stated that all money obtained was used to fund payroll, pay lease payments or truck expenses, and that no money was used for personal purposes.

22. Cawanza Wilkins, who received part of the PPP loan proceeds from Fayne, informed a Wells Fargo bank investigator that she was not an employee of Flame Trucking and that Fayne was her brother. After receiving a $350,000 wire transfer from Flame Trucking, which came out of the PPP loan proceeds, Wilkins stated that she made certain wire transfers at the direction of Fayne, including an $84,000 wire to Bank of America account 6871 to Status Jewelers in Duluth, Georgia, and a $40,000 wire transfer for child support completion to S.T. at Arkansas Federal Credit Union, account 9764.

23. On May 6, 2020, I obtained a seizure warrant from the United States District Court for any and all funds maintained in UCBI Account 1408. *See* 1:20-MJ-355.

24. On May 7, 2020, federal law enforcement agents interviewed Cawanza Wilkins. Wilkins stated she was not an employee of Flame Trucking and that Fayne was her "godbrother." Prior to receiving the $350,000 wire transfer from Flame Trucking on April 23, 2020, Fayne told Wilkins that he (Fayne) had received a COVID-19 loan from the U.S. Government and was sending her some of it so that she could handle payroll for him when he was not around. After receiving the $350,000 wire transfer from Fayne, Wilkins stated that she made certain wire transfers for payroll at the direction of Fayne, including an $84,000 wire to Status Jewelers in Duluth, Georgia, and a $40,000 wire transfer for to S.T. at Arkansas Federal Credit Union. Fayne told Wilkins both of these wire transactions were for payroll purposes.

25. The investigation has determined that the $40,000 wire transfer to S.T. on April 30, 2020 was for child support, and the $84,000 wire transfer to Status Jeweler on April 28, 2020 was for jewelry, specifically the three pieces of jewelry that I obtained seizure warrants for this morning in Case Number 1:20-MJ-361, those being the following:

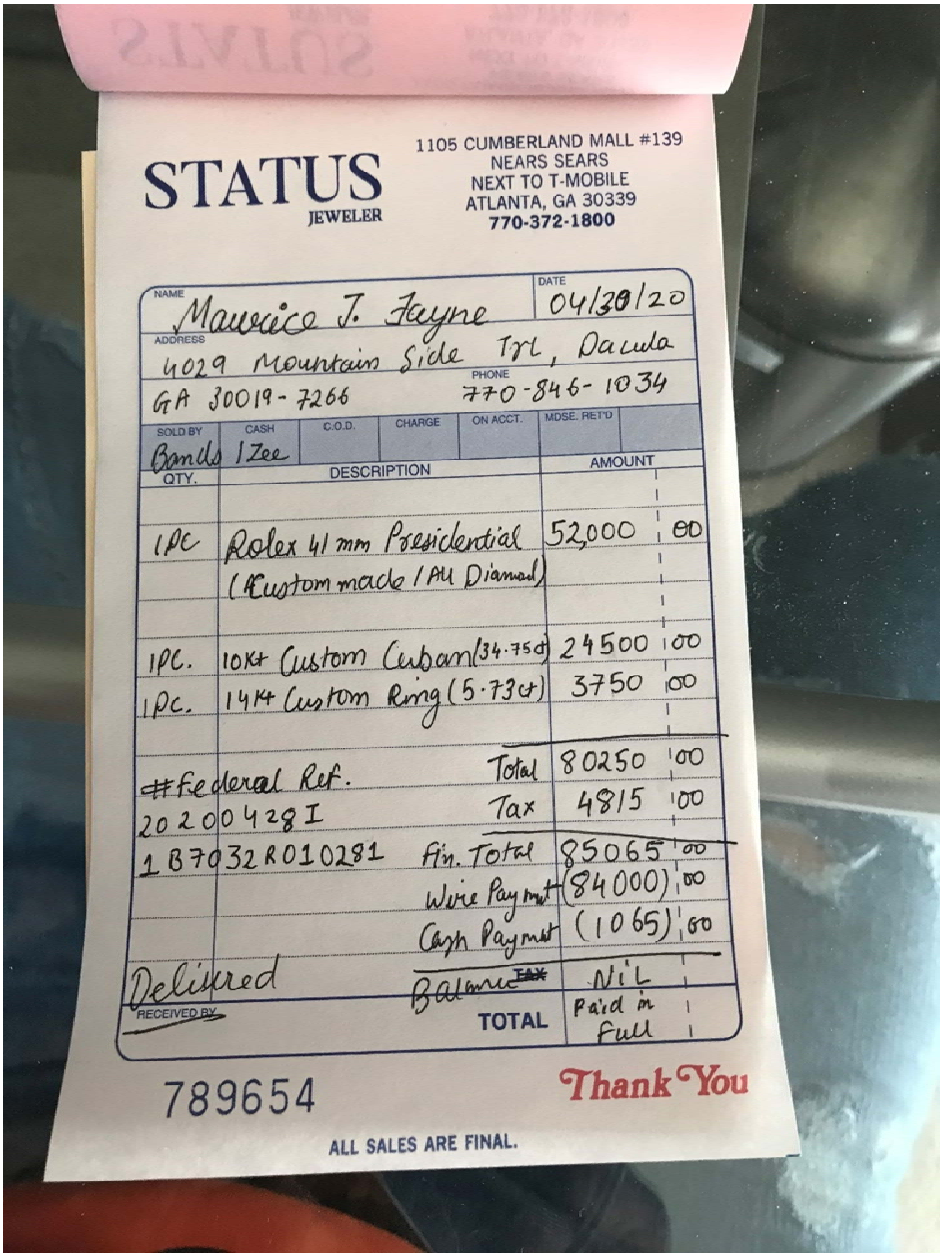
a. one custom-made 18 kt Rolex 41mm Presidential watch, serial number 5636S3S8, with diamonds, which sold for $52,000;

b. one 10 kt custom-made Cuban bracelet with 34.75 carats of diamonds, which sold for $24,500; and

c. one 14 kt custom-made ring with 5.73 carats of diamonds, which sold for $3,750.

26. Payments for jewelry and child support are not an authorized uses of PPP loan proceeds. *See* Federal Register /Vol. 85, No. 76 /Monday, April 20, 2020 /Rules and Regulations.

27. The above-described jewelry is listed in the following sales receipt that Status Jeweler issued to Fayne:



STATUS
JEWELER

1105 CUMBERLAND MALL #139
NEARS SEARS
NEXT TO T-MOBILE
ATLANTA, GA 30339
770-372-1800

NAME: Maurice J. Fayne
DATE: 04/30/20
ADDRESS: 4029 Mountain Side Trl, Dacula
GA 30019-7266
PHONE: 770-846-1034

SOLD BY	CASH	C.O.D.	CHARGE	ON ACCT.	MDSE. RET'D
Bonds / Zee					

QTY.	DESCRIPTION	AMOUNT
1Pc	Rolex 41 mm Presidential (Custom made / All Diamond)	52,000 00
1Pc.	10Kt Custom Cuban (34.75ct)	24500 00
1Pc.	14Kt Custom Ring (5.73ct)	3750 00
	Total	80250 00
#Federal Ref. 20200428I	Tax	4815 00
1B7032R010281	Fin. Total	85065 00
	Wire Payment	(84000) 00
	Cash Payment	(1065) 00
Delivered	Balance Due	NIL
RECEIVED BY	TOTAL	Paid in Full

789654

Thank You

ALL SALES ARE FINAL.

28. Records from Status Jeweler confirm that Fayne paid for the above-described jewelry with an $84,000 wire transfer plus $1,065 in cash, that the purchase was paid in full, and that the jewelry was delivered to Fayne at **the Subject Premises**.

29. A representative of Status Jeweler stated that the above-described jewelry was delivered to Fayne at **the Subject Premises** on three separate days. The watch was delivered on April 29, the bracelet was delivered on April 30, and the ring was delivered on May 1.

30. The following photograph shows Fayne wearing all three pieces of the jewelry, that is, the watch, the bracelet, and the ring:

Probable cause justifying seizure of electronic devices and electronically stored information ("ESI")

31. As mentioned above, the fraudulent bank statements for October, November, and December 2019 were submitted to UCBI through the use of the e-mail account flametruckinc@gmail.com.

32. Based on my training and experience, I know that a Gmail account is a Google account that offers users the ability to send and receive e-mail through an electronic device, such as a desktop computer, a tablet, a laptop, or a smartphone.

33. Based on my training and experience, I also know that computer software that operates on electronic devices, such as desktop computers, tablets, and laptops, can be used to create fictitious documents that appear to be authentic, such as the fraudulent bank statements that were submitted to UCBI.

34. Based on my training and experience, I am aware that those who use electronic devices for business purposes often store data on those devices, which can include, but is not limited to, email correspondence; financial and personal identification data, including bank account numbers, credit card numbers, and names, addresses, telephone numbers, and social security numbers; and/or records of financial transactions. Businesses like Flame Trucking, moreover, typically make use of accounting software to

track finances including payroll, expenses and accounts receivable, and customer relationship management software to keep track of customers and potential customers.

35. As described above and in Attachment B, this application seeks permission to search for records that might be found on **the Subject Premises**, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

36. *Probable cause.* I submit that if a computer or storage medium is found on **the Subject Premises**, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered

months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

e. Based on actual inspection of other evidence related to this investigation—the fraudulent bank statements—I believe that computer equipment was used to generate, store, and print documents used in the bank fraud scheme. As such, there is reason to believe that there is a computer system currently located on **the Subject Premises**.

37. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium located at **the Subject Premises** because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging

systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-

virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For

example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context,

draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

38. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on

storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from **the Subject Premises**, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks

or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on **the Subject Premises**. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

39. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant.

The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

Conclusion

40. For the reasons set forth above, I submit that there is probable cause to believe that Fayne violated the bank fraud statute, 18 U.S.C. § 1344, in two ways: first, by making false statements to UCBI in connection with Flame Trucking's PPP loan application; and second, by using proceeds from Flame Trucking's PPP loan to pay child support and purchase jewelry. In addition, I submit that there is probable cause to believe that Fayne's personal use of the PPP loan proceeds (to pay child support and purchase jewelry) violated the money laundering statutes, specifically 18 U.S.C. § 1956(a)(1)(B)(i) and 18 U.S.C. § 1957.

41. Since the jewelry that is the subject of my seizure warrants was delivered to **the Subject Premises** approximately one week ago, since it appears from the photograph that Fayne purchased the jewelry for himself, and since Fayne lives at **the Subject Premises**, I submit that it is reasonable to believe that the jewelry is currently located at **the Subject Premises**.

42. Since Flame Trucking's Principal Office is located at **the Subject Premises,** and since the Gmail account that Fayne used to send fraudulent bank statements to UCBI in support of Flame Trucking's fraudulent PPP loan application can only be accessed using an electronic device, such as a computer, a smartphone, or a tablet, I submit that it is reasonable to believe that one or more electronic devices are located at **the Subject Premises**.

43. I further submit that it is reasonable to believe that business records pertaining to Flame Trucking, records pertaining to the fraudulent PPP loan application Fayne submitted to UCBI in the name of Flame Trucking, and records pertaining to Fayne's illegal use of the PPP loan proceeds are stored on one or more electronic devices located at **the Subject Premises**.

44. I therefore request that the Court issue the proposed search warrant authorizing the search of the Subject Premises, as further described in Attachment A, for the things described in Attachment B.

Request for Sealing

45. I further request that the Court order that all papers in support of this application, including the affidavit and search warrants, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to the targets of the

investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee or continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, intimidate potential witnesses, notify confederates or otherwise seriously jeopardize the investigation.

Attachment A
Property to be Searched

The property to be searched is a residence located at 4029 Mountain Side Trail, Dacula, Georgia, 30019. It is depicted in the photographs below and is a two story, brown brick, five bedroom, three bathroom, approximately 4,170 square foot single family home with black shutters located in the Overlook subdivision in Dacula, Georgia. The front door is black with windows on the top half of the door. The three vehicle garage is brown and is on the left side of the home if it is faced from the roadway. **The Subject Premises** includes the residence, the garage, the curtilage, and outbuildings located at **the Subject Premises** or within its curtilage.

Attachment B

Property to be Seized

1. Records, in whatever format found, relating to violations of Title 18, United States Code, §§§ 1344 (Bank Fraud), 1956 (Money Laundering), 1957 (Transactional Money Laundering), and conspiracy to commit these offenses, involving MAURICE JOHNSON FAYNE, FLAME TRUCKING, CAWANZA WILKINS and others identified and/or unidentified, and occurring after April 4, 2019, including:

    a. Records, information, and/or communications related to the Small Business Administration and the Paycheck Protection Program;

    b. Records, information, and/or communications relating to bank accounts, loan accounts, credit card accounts, or other financial accounts, including, but not limited to, account numbers, credit and debit cards, records concerning the establishment, possession, access, and control of the accounts, wire transfers, deposits and other credits, debits and other withdrawals, monetary instruments, cashier's checks, personal checks, receipts, letters of credit, credit card statements, money orders, passbooks, cancelled checks,

certificates of deposit, loan records, income and expense summaries, and cash disbursement journals;

c. All tax records, including but not limited to state and federal individual and corporate tax returns;

d. Records, information, and communications relating to and reflecting FLAME TRUCKING, including, but not limited to, Secretary of State or other government office records, registration records, Articles of Incorporation and other incorporation documents, bank records, employment records, paychecks, paystubs, work schedules, records of and agreements with payroll processing companies, letterhead, email addresses, websites, and correspondence;

e. All communications, in any form, with or between MAURICE JOHNSON FAYNE and the following individuals: CAWANZA WILKINS, JONATHAN MARTIN, TYRICE VAUGHAN, GREAT DANE LLC, DANIEL JAY, TRANSAM TRUCKING EXCHANGE, CORNELIUS HOOD, MICHAEL SARGENT, JAMAAL SHEPARD, and JACQUELINE WOODS;

f. Lists of contacts and related identifying information for other co-conspirators, including, but not limited to, aliases, phone numbers, photographs, and social media;

g. Official checks, cashier's checks, money orders, United States currency, foreign currency, or any other monetary instruments;

h. Indicia of occupancy, residence, control or ownership of the SUBJECT PREMISES;

i. Records, information, and/or communications related to United Community Bank, Inc., including correspondence to and from the bank;

j. Records related to Arvest Bank, including bank statements;

k. Records related to flametruckinc@gmail.com;

l. Any documents, records, programs, or applications that identify the internet service provided to the SUBJECT PREMISES; and

m. Records and information establishing ownership and control over the seized items in paragraphs 2, 3, and 4.

2. 18 kt Rolex 41mm Presidential watch, serial number 5636S3S8, with diamonds.

3. 10 kt custom-made Cuban bracelet with 34.75 carats of diamonds.

4. 14 kt custom-made ring with 5.73 carats of diamonds.

5. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

h. evidence of the times the COMPUTER was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. records of or information about Internet Protocol addresses used by the COMPUTER;

l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and

m. contextual information necessary to understand the evidence described in this attachment.

6. Routers, modems, and network equipment used to connect computers to the Internet.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware. The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.